

Informe de Auditoría de Seguridad

Empresa X



8 de enero de 2023

Otra información



|  |  |
| --- | --- |
| Nombre del informe | Informe de auditoría de Enero 2023 |
| Fecha del informe | 2023-01-11 |
| Empresa | Google |
| Web de la Empresa | https://www.google.es |

AVISO LEGAL

Este documento contiene información confidencial y propietaria la cual es de uso exclusivo de **Google**. La reproducción o uso no autorizado de este documento está totalmente prohibida.

1. Índice

Añadir índice de Word

1. Introducción

Durante las pruebas se simulan las actividades que realizaría un atacante real, descubriendo las vulnerabilidades, su nivel de riesgo, y generando recomendaciones que permitan al cliente realizar la remediación de estas. En cada sección de este informe se detallan los aspectos importantes de la forma en que un atacante podría utilizar la vulnerabilidad para comprometer y obtener acceso no autorizado a información sensible. Se incluyen además directrices que al ser aplicadas mejoraran los niveles de confidencialidad, integridad y disponibilidad de los sistemas analizados.

* 1. Objetivo

El objetivo de la evaluación de seguridad es detectar las vulnerabilidades de seguridad existentes en los sistemas analizados para posteriormente generar un informe con los hallazgos y recomendaciones que permitan la remediación de estas.

* 1. Alcance

La evaluación realizada se ha centrado en los objetivos aprobados en el alcance del contrato, en el cual se establece:

* + Nombre: dc121 IP: 192.168.20.254
  + Nombre: google.es IP: 44.4.4.4
  + Nombre: SQL2023 IP: 10.10.10.5
  + Nombre: nginx01 IP: 10.10.10.4

1. Resultado de las pruebas

A continuación se detalla la información de cada activo analizado.

|  |  |
| --- | --- |
| Hostname | dc121 |
| IP | 192.168.20.254 |
| Descripción | Servidor DC principal |
| Sistema Operativo | Windows Server 2022 |
| Estado | El activo tiene vulnerabilidades. |
| Propuestas | Propuestas del activo |
| Recomendaciones | Recomendación del activo |

|  |  |
| --- | --- |
| Hostname | google.es |
| IP | 44.4.4.4 |
| Descripción | Web |
| Sistema Operativo | Apache |
| Estado | El activo tiene vulnerabilidades. |
| Propuestas |  |
| Recomendaciones |  |

|  |  |
| --- | --- |
| Hostname | SQL2023 |
| IP | 10.10.10.5 |
| Descripción | Servidor SQL principal |
| Sistema Operativo | Microsoft SQL 2023 |
| Estado | El activo no tiene vulnerabilidades. No se muestran propuestas ni recomendaciones |

|  |  |
| --- | --- |
| Hostname | nginx01 |
| IP | 10.10.10.4 |
| Descripción | Servidor Nginx |
| Sistema Operativo | nginx |
| Estado | El activo tiene vulnerabilidades. |
| Propuestas |  |
| Recomendaciones |  |

1. Recomendaciones

A continuación, se muestras las recomendaciones generales de la auditoría realizada

Recomendaciones generales del informe

* 1. Propuestas de mejora

A continuación, se muestran las propuestas de mejora tras la auditoría realizada.

Propuestas generales del informe

* 1. Tabla de vulnerabilidades y esfuerzos

Se muestran todas las vulnerabilidades, criticidad y esfuerzo para solventarlo

|  |  |  |  |
| --- | --- | --- | --- |
| CVE | Criticidad | Esfuerzo | Recomendación |
| CVE-2022-0778 | Muy Alta | Alto | Customers with a Threat Prevention subscription can block known attacks for this vulnerability by enabling Threat IDs 92409 and 92411 (Applications and Threats content update 8552). This mitigation reduces the risk of exploitation from known exploits.Customers will need to upgrade their products to a fixed version to completely remove the risk of this issue. |
| CVE-2022-32749 | Alta | Medio | Actualizar a la versión recomendada |
| CVE-2022-30209 | Alta | Alto | A complete vendor solution is available. Either the vendor has issued an official patch, or an upgrade is available. |
| CVE-2021-32588 | Muy Alta | Medio | Actualizar a la versión correspondiente |

1. Gráficas
   1. Gráfica de esfuerzos

El gráfico de esfuerzos sería el siguiente:

* 1. Gráfica de criticidades

El gráfico de criticidad sería el siguiente:

* 1. Gráfica OWASPtop10

El gráfico de vulnerabilidades en categorías OWASP sería el siguiente: